On the Theory of Rational Derivation on a Cubic Curve.

By William E. Story.

Theory of Indices.

In a recent number of this journal* Professor Sylvester has given the elements of a theory of *rational derivation* on a cubic curve, i. e. a theory of those points of the curve whose co-ordinates can be expressed as rational functions of an arbitrary *initial* point of the same; a theory which, although devised for the purpose of solving an arithmetical problem,† has an interest of its own from a geometrical point of view. It is, so far as it goes, the essence of the theory of the representation of the points on a cubic by means of a single parameter, i. e. its methods are substantially the same as those which have been employed in the development of that theory, but it does not assume any such actual representation. Previous to the above-mentioned foundation of this theory no one had ever, so far as I know, considered other rational derivatives of a point than its tangentials of various orders.

In this paper I propose to develop this new *theory of indices* in a more general and symmetrical form than that originally given to it; and, finally, by combining it with the theory of parameters, I shall solve a number of problems especially relating to the enumeration of points having certain properties analogous to those of singular points or of the contacts of singular tangents.

I shall call, with Professor Sylvester, the point in which the junction of two points of the cubic again meets the curve the *connective* of those two points; then it is evident that the connective of any two rational derivatives of a common initial point is also a rational derivative of the same initial. The tangential of a rational derivative is only a special case of such a connective, viz. the connective of the rational derivative with itself. It is by this method of collineation that Professor Sylvester obtains the derivatives. That such a method will give *all* the rational derivatives of a point is not yet proved, and the question is irrelevant to

---

* This volume, pages 58–88.

† Namely, from one solution in integers of the equation $x^3 + y^3 + z^3 + kxyz = 0$, to find others.

the present investigation; but, in view of the results obtained, it is difficult to see how any geometrical method can give other rational derivatives; at all events, I shall for the present use the expression *derivative* to designate such a derivative only. The derivatives which are thus obtained are the points to which correspond, as I shall show, values of the parameter differing only by multiples of certain periods (the inflexion-periods) from commensurable values, if the parameter μ be so chosen, as it always may be, that $\mu + \mu' + \mu'' = 0$ is the condition for three collinear points. The difference in method of the theories of *indices* and *parameters* consists in this: that in the latter continuous values of a parameter are assigned to the continuous points of the curve in accordance with its equation, while in the former to an arbitrary point taken as the initial an index 1 is assigned, and then to its derivatives in a certain order all positive and negative integers as indices. The index of a derivative thus expresses (with a certain modification due to the inflexion-periods) the number by which the parameter of the initial must be multiplied in order to obtain the parameter of the derivative. Viewed from an algebraic standpoint, as Professor Sylvester has shown, the square of the index of a derivative on a non-singular cubic is the degree of the co-ordinates of the derivative in terms of the initial; and from a geometrical standpoint, as is proved in the sequel, it is the number of points which bear to any given point the relation of initial to derivative with the index in question. This method of indices is particularly useful in determining the *number* of points whose derivatives satisfy certain conditions, and for such a determination it is in general necessary to take into account the periodicity of the parametric representation; at least it is necessary to distinguish the cases in which there is no period, or one or two periods. The advantage of considering the periodicity need not be lost in using the method of indices, so long as the problem in hand does not involve the actual determination of points, but only their number. If the question of reality enters, of course the nature of the periods and their relations to the co-ordinates must be considered. The condition of collineation above cited must be our guide in the assignment of the indices, in order that the relation mentioned may subsist between index and parameter,* i. e. for the indices a, b, c of three collinear points the fundamental formula holds,

$$a + b + c = 0,$$

* For the condition of collineation might have been chosen any linear relation between $a + b + c$, $bc + ca + ab$, abc and an arbitrary constant, i. e. any linear relation between the coefficients of the cubic equation of which a, b, c may be regarded as the roots; but it is more convenient to consider this condition as put, by a proper transformation, which is not in general algebraic, into the form given above. The indices of all the rational derivatives of any point will then be integers; otherwise they will be commensurable fractions.

or
$$[a\,,b] = -(a+b), \tag{1}$$
if, in general, $[a\,,b]$ denote the index of the connective of two points whose indices are a and b. In particular, for the tangential of a point whose index is a we have
$$[a\,,a] = -2\,a, \tag{2}$$
and for an inflexion
$$-2\,a = a, \text{ i. e. } a = 0, \tag{3}$$
so that each inflexion has the index 0. I shall have occasion hereafter to distinguish derivatives having a common index by means of suffices, but at present we will confine our attention to one point corresponding to each index, and to one inflexion selected at pleasure (a real inflexion, if we are to consider real derivatives) and give it the index 0, so that it will not yet be necessary to use any distinguishing mark. The connective of any point with an inflexion may be called the *opposite* of that point with respect to the inflexion. For the opposite with respect to 0 of a point whose index is a we have
$$[a\,,0] = -a. \tag{4}$$
We know that the opposites of three collinear points with respect to the same inflexion are also collinear; hence, if $[a\,,b] = -(a+b)$ for any particular values of a and b, then
$$[-a\,,-b] = (a+b). \tag{5}$$

It is necessary to show that the indices can be assigned so that the fundamental formula (1) shall hold for any two derivatives and their connective. The application of (4) and (5) will make it unnecessary to prove the formula separately for all cases; viz., every number of the form $3\,m-1$, in which m is any positive or negative integer, is the negative of a number of the form $3\,m+1$; after I have assigned all the indices of the form $3\,m+1$, I shall assign those of the form $3\,m-1$ by (4); and when the fundamental formula has been proved for the connective of any two indices of the form $3\,m+1$, it is shown by (5) to hold for two indices of the form $3\,m-1$. It will be noticed that, if a and b are both of one of the forms $3\,m+1$, $3\,m-1$, $3m$, then $-(a+b)$ is also of that form; and if a and b are of different forms, $-(a+b)$ is of the form different from either.

The proof of the fundamental formula, after the indices have been assigned, depends upon a special form of a theorem of Professor Sylvester's (Salmon's Higher Plane Curves, 2d ed., page 135), which may be put thus: *If four points on a cubic be grouped in pairs in any way, the connective of the connectives of the points in the separate pairs is independent of the manner of grouping.* The point which thus

depends only on the position of the four given points is their *coresidual*, and its index may be denoted by $[a, b, c, d]$, where a, b, c, d are the indices of the four points. The theorem just stated may then be expressed thus:—

$$\big[[a,b],[c,d]\big] = \big[[a,c],[b,d]\big] = \big[[a,d],[b,c]\big] = [a,b,c,d]. \qquad (6)$$

For convenience I omit the inside brackets and write the indices in the order in which they are used in pairs, separating them by commas; thus (6) becomes

$$[a,b,c,d] = [a,c,b,d] = [a,d,b,c].$$

Later I shall speak also of the coresidual of $3n+1$ indices instead of the index of the coresidual of $3n+1$ points. The indices of the form $3n+1$ are assigned thus:—

$$1 = \text{index of the initial},$$

$$[1,1] = -2 = \text{index of the tangential of the initial},$$

and then, by the use of -2 and 1 alternately,

$$\begin{array}{ll} [-2,-2] = 4, & [4,1] = -5, \\ [-5,-2] = 7, & [7,1] = -8, \\ [-8,-2] = 10, & [10,1] = -11, \text{ etc.,} \end{array}$$

from which follow

$$\begin{array}{ll} & [-2,1] = 1, \\ [4,-2] = -2, & [-5,1] = 4, \\ [7,-2] = -5, & [-8,1] = 7, \\ [10,-2] = -8, & [-11,1] = 10, \text{ etc.,} \end{array}$$

so that, if a is any index of the form $3m+1$,

$$[a,1] = -(a+1) \quad \text{and} \quad [a,-2] = -(a-2). \qquad (7)$$

If a and b are any two indices of the form $3m+1$, then by (7) and (6)

$$\begin{aligned} [a,b] &= [-(a+1), 1-(b-2), -2] = [-(a+1), -2, -(b-2), 1] \\ &= [a+3, b-3], \qquad (8) \end{aligned}$$

so that the index of the connective* of two indices remains unchanged if either index be increased by any multiple of 3, while the other is decreased by the

* It is a convenient abbreviation to speak of the connective of two *indices* instead of that of the corresponding points.

same multiple of 3, the sum remaining constant. Whatever value $\equiv 1 \pmod{3}$ either index may have, it can be increased if negative, or decreased if positive, by such a multiple of 3 that it shall become 1, so that (a and b both of the form $3m+1$)

$$[a, b] = [a+b-1, 1] = -(a+b);$$

and hence by (5)

$$[-a, -b] = (a+b),$$

i.e. the fundamental formula holds for any two indices, both of the form $3m+1$, or both of the form $3m-1$. I will introduce multiples of 3 by the formula

$$[3m-1, 1] = -3m, \tag{9}$$

for all positive and negative values of m, in accordance with the fundamental theorem. Then also, for all values of m,

$$[3m, 1] = -(3m+1). \tag{10}$$

Then by (1), (4), (6), and (9), of which (1) and (4) are now known to be true for indices of the form $3m+1$ and of the form $3m-1$,

$$[3m+1, -1] = [-3m+1, -2, 1, 0] = [-3m+1, 0, -2, 1] = [3m-1, 1] \\ = -3m, \tag{11}$$

from which follows

$$[3m, -1] = -(3m-1). \tag{12}$$

Moreover

$$[3m, 0] = [-3m+1, -1, 0, 0] = [-3m+1, 0, -1, 0] = [3m-1, 1] \\ = -3m. \tag{13}$$

It has now been proved that, for *all* values of a,

$$[a, 1] = -(a+1), \quad [a, -1] = -(a-1), \quad \text{and} \quad [a, 0] = -a; \tag{14}$$

whence, for *all* values of a and b,

$$[a,b]=[-a-1,1,-b+1,-1]=[-a-1,-1,-b+1,1]=[a+2,b-2], \tag{15}$$

which can be repeated any number of times until one or the other of the two indices becomes 0 or 1, in either of which cases the fundamental formula holds; hence it holds for all values of a and b, i.e.

I. *The connective of any two indices is their negative sum.*

For the coresidual of four indices a, b, c, d we have

$$[a, b, c, d] = [-a-b, -c-d] = a+b+c+d, \tag{16}$$

i. e.,

II. *The coresidual of four indices is their sum.*

In general (see Salmon's Higher Plane Curves, 2d ed., §§ 154 – 161), given any $3n-1$ points on a cubic, all the curves of the order n which can be passed through them will intersect the cubic again in a fixed point, the *residual* of the given $3n-1$ points; and given any $3n+1$ points on a cubic, any curve of the order $n+1$ which can be passed through them will intersect the cubic again in two points whose connective is a fixed point, the *coresidual* of the given $3n+1$ points. Furthermore it is substantially proved (Salmon, l. c.) that, in the determination of residual or coresidual, for any group of $3k+1$ points can be substituted their coresidual; hence, in the determination of the index of the residual or coresidual of any number of points of the numbered scale, for any four indices we may substitute their sum. We may then group the given indices together by fours as far as possible, and substitute for each four their sum, thus reducing the number of indices by a multiple of 3, without altering their sum. The same reduction may be made in the system of indices thus obtained, and this process carried on until the number of indices is less than four. We speak only of a *residual* of $3n-1$ points and the *coresidual* of $3n+1$ points; so that, after the above reduction in the number of points by a multiple of 3, there will result two points whose residual is their negative sum, or a single point which is the coresidual of the given $3n+1$ points. Hence

III. *The residual of any* $3\mathrm{n}-1$ *indices is their negative sum, and the coresidual of any* $3\mathrm{n}+1$ *indices is their sum.*

It may be added that the sum of any $3n-1$ indices is the coresidual of the group formed by annexing to them the inflexion 0 twice; the negative sum of any $3n+1$ indices is the residual of the group formed by annexing to them the inflexion 0; the sum of any $3n$ indices is the coresidual of the group formed by annexing to them the inflexion 0; and the negative sum of $3n$ indices is the residual of the group formed by annexing to them the inflexion 0 twice, i. e. is the $3(n+1)^{\text{th}}$ intersection with the cubic of every curve of the order $n+1$ which passes through the $3n$ points, and is tangent to the cubic at the inflexion 0.

Theorem II. can be put into this simple form: *The sum of the indices of the* $3\mathrm{n}$ *points of intersection of any* n*-thic with the cubic is* 0.*

* Compare Clebsch, *Vorlesungen über Geometrie*, edited by Lindemann, Vol. I. p. 623.

The foregoing is the complete theory for cuspidal cubics, which have only one point of inflexion; but on a cubic having more than one inflexion, a series of derivatives whose indices are of the form $3m$ and $3m-1$ exists for each inflexion, and these series determine by collineation yet other series whose indices are of the form $3m+1$.

An acnodal or crunodal cubic will have three collinear inflexions; let their indices be $0_0, 0_1, 0_2$ (the numerical value of the index of any inflexion is 0, as above proved); let the indices a_0, for all integral values of a, be assigned as in the preceding case the indices a were, i.e. let 1_0 be the index of any point on the curve, let $-2_0, 4_0, -5_0, 7_0, \ldots.$ be assigned with respect to 1_0 as $-2, 4, -5, 7, \ldots.$ were assigned with respect to 1, and let $-1_0, 2_0, -4_0, 5_0, \ldots.$ be assigned with respect to 1_0 and 0_0 as above $-1, 2, 3, -3, -4, 8, \ldots.$ were with respect to 1 and 0. Further, let

$$[a_0, 0_2] = -a_1 \quad \text{and} \quad [a_0, 0_1] = -a_2 \tag{17}$$

serve for the assignment of all indices with the suffices 1 and 2. Then, for all values of a and b,

$$[0_0, 0_0] = 0_0, [0_1, 0_1] = 0_1, [0_2, 0_2] = 0_2,$$

$$[0_1, 0_2] = 0_0, [0_2, 0_0] = 0_1, [0_0, 0_1] = 0_2,$$

$$[a_0, b_0] = -(a+b)_0,$$

$$[a_1, b_2] = [-a_0, 0_2, -b_0, 0_1] = [-a_0, -b_0, 0_1, 0_2] = [(a+b)_0, 0_0] = -(a+b)_0,$$

$$[a_2, b_0] = [-a_0, 0_1, -b_0, 0_0] = [-a_0, -b_0, 0_0, 0_1] = [(a+b)_0, 0_2] = -(a+b)_1,$$

$$[a_0, b_1] = [-a_0, 0_0, -b_0, 0_2] = [-a_0, -b_0, 0_2, 0_0] = [(a+b)_0, 0_1] = -(a+b)_2,$$

$$[a_1, b_1] = [-a_0, 0_2, -b_0, 0_2] = [-a_0, -b_0, 0_2, 0_2] = [(a+b)_0, 0_2] = -(a+b)_1,$$

$$[a_2, b_2] = [-a_0, 0_1, -b_0, 0_1] = [-a_0, -b_0, 0_1, 0_1] = [(a+b)_0, 0_1] = -(a+b)_2;$$

so that, in general, if $\rho(x)$ denotes the minimum positive residue of x (mod. 3), we shall have

$$[a_p, b_q] = -(a+b)_{\rho[-(p+q)]}, \tag{18}$$

where each of the numbers p and q has one of the values 0, 1, 2. Evidently then

$$\begin{aligned}[a_p, b_q, c_r, d_s] &= [-(a+b)_{\rho[-(p+q)]}, -(c+d)_{\rho[-(r+s)]}] \\ &= [a+b+c+d]_{\rho(p+q+r+s)}.\end{aligned} \tag{19}$$

By a simple extension of these formulæ, as in the case of the cuspidal cubic, to the residual or coresidual of any number of points, we have

IV. *The residual of any* $3\,n - 1$ *indices on a crunodal or acnodal cubic is their negative sum with a suffix equal to the minimum positive residue* (*mod.* 3) *of the negative sum of their suffices; and the coresidual of any* $3\,n + 1$ *indices on such a cubic is the sum of their indices with a suffix equal to the minimum positive residue* (*mod.* 3) *of the sum of their suffices.*

The presence of an inflexion in a group of derivatives can only affect the number of indices in the group and the suffix of the resultant index, i. e. can only have an effect in determining whether the result is residual or coresidual, and hence whether the sum of the indices and the sum of the suffices are to be taken with the positive or negative sign. With this in mind it is easy to make additions to the theorem just given analogous to those which we made to Theorem II., respecting the meaning of the positive sum of $3\,n - 1$ indices, the negative sum of $3\,n + 1$ indices, and the positive and negative sums of $3\,n$ indices, each with either possible suffix. For instance, the sum of $3\,n$ indices with a suffix equal to the minimum positive residue (mod. 3) of the sum of their suffices is the coresidual of the group formed by annexing to the given $3\,n$ points the inflexion 0_0; the same sum with a suffix one greater (mod. 3) is the coresidual of the group formed by annexing to the $3\,n$ points the inflexion 0_1; the negative sum of $3\,n$ indices with a suffix equal to the minimum positive residue (mod. 3) of the negative of the sum of their suffices is the $3\,(n+1)^{\text{th}}$ point of intersection with the cubic of every curve of the order $n+1$, which passes through the $3\,n$ given points and touches the cubic at the point of inflexion 0_0, and also of every curve of the same order which passes through the $3\,n$ given points and through the inflexions 0_1 and 0_2; the same index with the suffix increased by 1 will be that of the point of intersection when 0_1 is the point of contact or the curve passes through 0_0 and 0_2, etc.

These theorems are true for the derivatives obtained by means of any three collinear inflexions, if three or more exist, and will therefore be true for non-singular cubics as well as for acnodal and crunodal cubics. Non-singular cubics have nine points of inflexion lying by threes in twelve straight lines; designating any three inflexions which are not collinear by 0_{00}, 0_{01}, 0_{10}, in accordance with the above principles I will assign double indices to each of the other six inflexions (using only 0, 1, 2 as suffices) so that the conditions of collineation for $0_{p,q}$, $0_{r,s}$, $0_{t,u}$ shall be $p + r + t = 0$ and $q + s + u = 0$, or, using $\rho(x)$ as above,

$$[0_{p,q}\,,\, 0_{r,s}] = 0_{\rho[\;\;(p+r)],\rho[-(q+s)]}.$$

The twelve sets of collinear inflexions are then

$$\begin{array}{llll} 0_{00}, 0_{01}, 0_{02}; & 0_{00}, 0_{10}, 0_{20}; & 0_{01}, 0_{10}, 0_{22}; & 0_{01}, 0_{20}, 0_{12}; \\ 0_{10}, 0_{02}, 0_{21}; & 0_{10}, 0_{12}, 0_{11}; & 0_{02}, 0_{20}, 0_{11}; & 0_{02}, 0_{22}, 0_{12}; \\ 0_{20}, 0_{22}, 0_{21}; & 0_{22}, 0_{00}, 0_{11}; & 0_{12}, 0_{00}, 0_{21}; & 0_{21}, 0_{01}, 0_{11}; \end{array} \tag{20}$$

namely, 0_{02}, 0_{20}, 0_{22}, 0_{12}, 0_{21}, 0_{11} are assigned successively by the first six collineations, and the other six follow, thus:—

$$\begin{aligned} [0_{02}, 0_{20}] &= [0_{00}, 0_{01}, 0_{20}, 0_{20}] = [0_{00}, 0_{20}, 0_{01}, 0_{20}] = [0_{10}, 0_{12}] = 0_{11}, \\ [0_{02}, 0_{22}] &= [0_{00}, 0_{01}, 0_{01}, 0_{10}] = [0_{01}, 0_{01}, 0_{00}, 0_{10}] = [0_{01}, 0_{20}] = 0_{12}, \\ [0_{20}, 0_{22}] &= [0_{00}, 0_{10}, 0_{01}, 0_{10}] = [0_{10}, 0_{10}, 0_{00}, 0_{01}] = [0_{10}, 0_{02}] = 0_{21}, \\ [0_{22}, 0_{00}] &= [0_{01}, 0_{10}, 0_{10}, 0_{20}] = [0_{10}, 0_{10}, 0_{01}, 0_{20}] = [0_{10}, 0_{12}] = 0_{11}, \\ [0_{12}, 0_{00}] &= [0_{01}, 0_{20}, 0_{00}, 0_{00}] = [0_{00}, 0_{20}, 0_{00}, 0_{01}] = [0_{10}, 0_{02}] = 0_{21}, \\ [0_{21}, 0_{01}] &= [0_{10}, 0_{02}, 0_{01}, 0_{01}] = [0_{10}, 0_{01}, 0_{01}, 0_{02}] = [0_{22}, 0_{00}] = 0_{11}. \end{aligned}$$

What I have represented in the preceding case by 0_0, 0_1, 0_2, a_0, a_1, a_2, I will represent in the case of the non-singular cubic by 0_{00}, 0_{10}, 0_{20}, a_{00}, a_{10}, a_{20}, respectively. Then, by (18) and (19),

$$[a_{p,0}, b_{r,0}] = -(a+b)_{\rho[-(p+r)],0}, \tag{21}$$

$$[a_{p,0}, b_{r,0}, c_{t,0}, d_{v,0}] = (a+b+c+d)_{\rho(p+r+t+v),0}. \tag{22}$$

Introducing $a_{p,1}$ and $a_{p,2}$ (where $p = 0$, 1, or 2) by the formula

$$a_{p,1} = [-a_{\rho(-p),0}, 0_{02}], \qquad a_{p,2} = [-a_{\rho(-p),0}, 0_{01}], \tag{23}$$

we have

$$\begin{aligned} [a_{p,1}, b_{r,1}] &= [-a_{\rho(-p),0}, 0_{02}, -b_{\rho(-r),0}, 0_{02}] = [(a+b)_{\rho(p+r),0}, 0_{02}] \\ &= -(a+b)_{\rho[-(p+r)],1}, \\ [a_{p,2}, b_{r,2}] &= [-a_{\rho(-p),0}, 0_{01}, -b_{\rho(-r),0}, 0_{01}] = [(a+b)_{\rho(p+r),0}, 0_{01}] \\ &= -(a+b)_{\rho[-(p+r)],2}, \\ [a_{p,1}, b_{r,2}] &= [-a_{\rho(-p),0}, 0_{02}, -b_{\rho(-r),0}, 0_{01}] = [(a+b)_{\rho(p+r),0}, 0_{00}] \\ &= -(a+b)_{\rho[-(p+r)],0}, \\ [a_{p,2}, b_{r,0}] &= [-a_{\rho(-p),0}, 0_{01}, -b_{\rho(-r),0}, 0_{00}] = [(a+b)_{\rho(p+r),0}, 0_{02}] \\ &= -(a+b)_{\rho[-(p+r)],1}, \\ [a_{p,0}, b_{r,1}] &= [-a_{\rho(-p),0}, 0_{00}, -b_{\rho(-r),0}, 0_{02}] = [(a+b)_{\rho(p+r),0}, 0_{01}] \\ &= -(a+b)_{\rho[-(p+r)],2}; \end{aligned}$$

i. e. in general

$$[a_{p,q}\,, b_{r,s}] = -\,(a+b)_{\rho[-(p+r)],\,\rho[-(q+s)]}\,. \qquad (24)$$

From this follows

$$[a_{p,q}\,, b_{r,s}\,, c_{t,u}\,, d_{v,w}] = [-\,(a+b)_{\rho[-(p+r)],\,\rho[-(q+s)]}\,, -\,(c+d)_{\rho[-(t+v)],\,\rho[-(u+w)]}]$$
$$= (a+b+c+d)_{\rho(p+r+t+v),\,\rho(q+s+u+w)}\,; \qquad (25)$$

and hence, by a process similar to that employed in the previous cases,—

IV. *The residual of any* $3\,\mathrm{n}-1$ *indices on a non-singular cubic is their negative sum with first and second suffices equal to the minimum positive residues (mod. 3) of the negative sums of their first and second suffices, respectively; and the coresidual of any* $3\,\mathrm{n}+1$ *indices on such a cubic is their sum with first and second suffices equal to the minimum positive residues (mod. 3) of the sums of their first and second suffices, respectively.*

An extension to the sum of $3n-1$, the negative sum of $3n+1$, and the positive and negative sums of $3n$ indices, with the various combinations of suffices, may be made here, as in the previous cases.

Compound Derivation.

The problem of compound derivation is to determine the point which is derived from a given derivative just as a certain other derivative is obtained from the initial. For instance, to determine the a of b is to determine the index which is derived from b just as a is from 1, where a and b may have any suffices in accordance with the notation already employed. In forming the derivatives of b, evidently the same operations (additions and changes of sign) are performed as in forming the derivatives of 1; the only difference is, that in the former case they are applied to multiples of b, but in the latter case to the same multiples of 1. Hence the numerical value of a of b is a times the numerical value of b, i. e. is ab, to which, if necessary, proper suffices must be given; and the problem really reduces to that of finding the suffices of the compound derivative when those of the components are known.

In the case of a cuspidal cubic there is only one point of inflexion, no indices are necessary, and, for all values of a and b,

$$a \text{ of } b = ab. \qquad (26)$$

In the case of an acnodal or crunodal cubic only one set of suffices is necessary, and evidently

$$a_0 \text{ of } b_p = (ab)_p, \qquad (27)$$

if a is of the form $3m+1$, b is any integer, and p is either 0, 1, or 2. If a is of the form $3m-1$, $-a$ is of the form $3m+1$, and hence

$$a_0 \text{ of } b_p = [-a_0 \text{ of } b_p, 0_0] = [-(ab)_p, 0_0] = (ab)_{\rho(-p)}. \tag{28}$$

If a is of the form $3m$, $-(a-1)$ is of the form $3m+1$ and -1 of the form $3m-1$, and hence

$$\begin{aligned} a_0 \text{ of } b_p &= [-(a-1)_0 \text{ of } b_p, -1 \text{ of } b_p] \\ &= [-\{(a-1)b\}_p, -b_{\rho(-p)}] = (ab)_0; \end{aligned} \tag{29}$$

so that, for all values of a, b, and p,

$$a_0 \text{ of } b_p = (ab)_{\rho(ap)}. \tag{30}$$

Hence, for all values of a, b, p, and q,

$$a_p \text{ of } b_q = [-a_0 \text{ of } b_q, 0_{\rho(-p)}] = [-(ab)_{\rho(-aq)}, 0_{\rho(-p)}] = (ab)_{\rho(p+aq)}. \tag{31}$$

In the case of the non-singular cubic there are two sets of suffices, and evidently

$$a_{00} \text{ of } b_{p,q} = (ab)_{p,q}, \tag{32}$$

if a is of the form $3m+1$; while, if a is of the form $3m-1$, and therefore $-a$ of the form $3m+1$,

$$a_{00} \text{ of } b_{p,q} = [-a_{00} \text{ of } b_{p,q}, 0_{00}] = [-(ab)_{p,q}, 0_{00}] = (ab)_{\rho(-p),\rho(-q)}; \tag{33}$$

but if a is of the form $3m$, $-(a-1)$ is of the form $3m+1$ and -1 of the form $3m-1$, and hence

$$\begin{aligned} a_{00} \text{ of } b_{p,q} &= [-(a-1)_{00} \text{ of } b_{p,q}, -1_{00} \text{ of } b_{p,q}] \\ &= [-\{(a-1)b\}_{p,q}, -b_{\rho(-p),\rho(-q)}] = (ab)_{00}; \end{aligned} \tag{34}$$

so that, for all values of a, b, p, and q,

$$a_{00} \text{ of } b_{p,q} = (ab)_{\rho(ap),\rho(aq)}. \tag{35}$$

From this follows, for all values of a, b, p, q, r, and s,

$$\begin{aligned} a_{p,q} \text{ of } b_{r,s} &= [-a_{00} \text{ of } b_{r,s}, 0_{\rho(-p),\rho(-q)}] \\ &= [-(ab)_{\rho(-ar),\rho(-as)}, 0_{\rho(-p),\rho(-q)}] \\ &= (ab)_{\rho(p+ar),\rho(q+as)}. \end{aligned} \tag{36}$$

The series of derivatives with indices of the form $3m+1$, without suffix, with suffix 0, or with suffices 00, i. e. the series of derivatives in whose determination no inflexion is employed, is called by Professor Sylvester the "natural scale" of

derivatives of the initial. Such a system is a closed system, i. e. the connective of any two natural derivatives of a point is also a natural derivative of that point. The natural scale taken with either series of indices of the form $3m-1$ and a certain series of indices of the form $3m$ constitutes a closed system. For example, the three series $(3m+1)_0$, $(3m-1)_1$, $(3m)_2$ constitute a closed system, as also $(3m+1)_{00}$, $(3m-1)_{12}$, $(3m)_{21}$. In fact, if p, q, r are the numbers 0, 1, 2 in any order, and s, t, u the same numbers in any order, then $(3m+1)_{p,s}$, $(3m-1)_{q,t}$, $(3m)_{r,u}$ constitute a closed system.

If real derivatives alone are to be considered, the system of indices without a suffix may be employed for crunodal as well as cuspidal cubics, and that with one suffix for non-singular as well as acnodal cubics. Indeed, if account is taken only of the closed system $(3m+1)_{p,s}$, $(3m-1)_{q,t}$, $(3m)_{r,u}$, there is no necessity for writing the indices, of which the form $3m+1$, $3m-1$, or $3m$ gives sufficient indication.

The system without suffices is to be regarded as included in that with one suffix, which is itself a special case of that with two suffices; and it will be convenient in the sequel to give every index two suffices, supplying 0 in place of each missing suffix; thus what I have heretofore denoted by a will now be denoted by a_{00}, and that heretofore denoted by a_p will be denoted by $a_{p,0}$ or $a_{0,p}$. Some agreement must be made as to the manner of supplying the missing suffix when only one is expressed, and this will affect in some degree the application of the theory of suffices to that of parameters, about which I shall presently say more.

The system above given without a suffix, as applied to non-singular cubics, is the only one explicitly treated by Professor Sylvester, who actually expresses the co-ordinates of such derivatives as rational algebraic functions, and from these expressions proves that the degree of the co-ordinates of the a^{th} derivative of any initial in the co-ordinates of the initial is the square of the numerical value of a,* and from this he infers that the number of a^{th} subderivatives of any point of the cubic (i. e. the number of points of which the given point may be considered as derivative with the index a) is a^2. This theorem is only true of non-singular cubics, and the proof seems to be wanting that every point obtained by equating to given values the co-ordinates of the derivative in terms of the initial is a point of the cubic. In so far as the theorem is true it holds also in the notation of this paper, inasmuch as the absolute numerical value of the index of any given derivative is the same in my notation as in Professor Sylvester's. This missing step is made good in the sequel.

---

* See pages 184–189.

Application of the Theory of Indices to that of Parameters.

The co-ordinates of any point of a cubic can be expressed as functions (rational or irrational) of a single parameter, which functions are either non-periodic, singly periodic, or doubly periodic;* so that we can classify cubics as *non-periodic* (cuspidal), *singly periodic* (acnodal or crunodal), and *doubly periodic* (non-singular). The non-periodic functions are algebraic; the singly periodic either trigonometric with a real period ∂,† or exponential with an imaginary period $2i\partial$; and the doubly periodic functions are elliptic with a real period $2K$ and an imaginary period $2iK'$.‡

Let ω, ω' denote the periods of the cubic, of which, say for convenience, ω is real and ω' is imaginary. Let also (μ) denote the point to which corresponds the value μ of the parameter, and let the sign $\equiv$, if the modulus is not expressed, denote equality, congruity (mod. ω), congruity (mod. ω'), or congruity (mod. ω, ω'), according as the curve is non-periodic, singly periodic with real period ω, singly periodic with imaginary period ω', or doubly periodic with real period ω and imaginary period ω'. Then the condition that three points (μ), (μ'), (μ'') shall be collinear is

$$\mu + \mu' + \mu'' \equiv 0, \tag{37}$$

i.e. the parameters of collinear points satisfy a congruence similar to the equations satisfied by the indices of three collinear derivatives of a common initial. Hence, if a is any integer of the form $3m + 1$,

$$a_{00} \text{ of } (\mu) = (a\mu). \tag{38}$$

---

* This representation of the singular cubics seems to be due to Salmon (Higher Plane Curves, 1st ed., 1852, Arts. 177, 178, and 183); and that of the non-singular cubics to Clebsch (Ueber einen Satz von Steiner und einige Punkte der Theorie der Curven dritter Ordnung, Crelle's Journal, Vol. LXIII., 1864). For a more thorough and systematic treatment, see Durège, Ueber fortgesetztes Tangentenziehen an Curven dritter Ordnung mit einem Doppel- oder Rückkehrpunkte, Math. Annalen, Vol. I. pp. 509–532; and Clebsch, Vorlesungen über Geometrie (herausgegeben von Lindemann), Vol. I. pp. 602–660. For further references, see Bibliography at the end of this article.

† I use the sign ∂ to denote the ratio of the circumference of a circle to its diameter, usually represented by π, and the reversed sign $\mathfrak{G}$ to denote the base of the natural system of logarithms.

‡ With the usual notation K and K' are the complete integrals of the first kind corresponding to the modulus k and its complementary k'.

The simplest representation seems to be the following, in which x, y, z denote the homogeneous co-ordinates of any point of the cubic:—

For a cuspidal cubic,	$x : y : z = \mu : 1 : \mu^3$,
For an acnodal cubic,	$x : y : z = \sin\mu : \cos\mu : \sin^3\mu$,
For a crunodal cubic,	$x : y : z = \mathfrak{G}^{\mu} : \mathfrak{G}^{2\mu} : 1 - \mathfrak{G}^{3\mu}$,
For a non-singular cubic,	$x : y : z = \operatorname{sn}\mu : \operatorname{cn}\mu \,.\, \operatorname{dn}\mu : \operatorname{sn}^3\mu$.

From (37) follows that the parameters corresponding to the inflexions are the solution of the congruence

$$3\mu \equiv 0,$$

i. e. for a non-periodic cubic, $\mu = 0$;

for a singly periodic cubic, $\mu \equiv 0, \frac{1}{3}\omega, \frac{2}{3}\omega$;

for a doubly periodic cubic,
$$\begin{array}{lll} \mu \equiv 0, & \frac{1}{3}\omega, & \frac{2}{3}\omega, \\ \frac{1}{3}\omega', & \frac{1}{3}\omega + \frac{1}{3}\omega', & \frac{2}{3}\omega + \frac{1}{3}\omega', \\ \frac{2}{3}\omega', & \frac{1}{3}\omega + \frac{2}{3}\omega', & \frac{2}{3}\omega + \frac{2}{3}\omega'. \end{array}$$

So that, in general, say,

$$0_{p,q} = p \cdot \tfrac{1}{3}\omega + q \cdot \tfrac{1}{3}\omega'. \tag{39}$$

From (24), (38), and (39) follows

$$\begin{aligned} a_{p,q} \text{ of } (\mu) &= [-a_{0,0} \text{ of } (\mu), 0_{\rho(-p),\rho(-q)}] = [(-a\mu), (-p \cdot \tfrac{1}{3}\omega - q \cdot \tfrac{1}{3}\omega')] \\ &= (a\mu + p \cdot \tfrac{1}{3}\omega + q \cdot \tfrac{1}{3}\omega'). \end{aligned} \tag{40}$$

From (39) and (40) follows that the first suffix of any index refers to the real and the second to the imaginary period; hence, in supplying a missing suffix, the new suffix 0 must be made the second or first according as the existing period is real or imaginary.

From the expressions for the co-ordinates given in the third footnote on page 368, it is evident that the necessary and sufficient condition for the reality of the point corresponding to a value μ of the parameter is

$$\mu \equiv \nu \,(\text{mod.}\ \tfrac{1}{2}\omega'), \tag{41}$$

where ν is real, which is equivalent to the condition that either μ is real or its imaginary part is half the imaginary period; if there is no imaginary period the parameter is real.

From (40) it is evident that any point whose parameter differs from an integral multiple of the parameter of a given point by integral multiples of the periods of the inflexions (which are $\frac{1}{3}\omega$ and $\frac{1}{3}\omega'$) is a rational derivative of the given point. In this sense *the theory of rational derivatives is the theory of commensurable parameters.*

The only real derivatives of a real point are evidently, from (40) and (41), those whose index has its second suffix 0, i. e. is of the form $a_{p,0}$, and every such derivative of a real point is real.

If (λ) is the $a_{p,q}$ of (μ),

$$\lambda \equiv a\mu + \tfrac{1}{3}(p\omega + q\omega'), \tag{42}$$

from which follows

$$\mu \equiv \frac{3\lambda + (3m - p)\,\omega + (3m' - q)\,\omega'}{3a}, \tag{43}$$

where each of the numbers m, m' is any integer less than $\pm a$* (including 0). The number of such sub-$a_{p,q}$'s of any point λ is thus evidently 1, $\pm a$, or a^2, according as the curve is non-periodic, singly periodic, or doubly periodic. For the doubly periodic or non-singular cubics this is Professor Sylvester's "law of squares." From the fact that the parameters given by (43) are all incongruent follows that the number of subderivatives of a given index is in *all* cases that just stated.

Moreover, it is evident from the formula that, *in general*, a point (μ) will not be at once a sub-$a_{p,q}$ and a sub-$b_{r,s}$ of the same point (λ), if b, r, s have other values than a, b, q respectively. There will, however, be points on the cubic, of which a subderivative with given index $b_{r,s}$ coincides with a subderivative with given index $a_{p,q}$, if a and b are different. To determine them, suppose (λ) to be a point of which a sub-$a_{p,q}$, say (μ), coincides with a sub-$b_{r,s}$, where for convenience we will suppose $a > b$; then (λ) is at once an $a_{p,q}$ of (μ) and a $b_{r,s}$ of (μ); hence

$$\lambda = a\mu + \tfrac{1}{3}(p\omega + q\omega') = b\mu + \tfrac{1}{3}(r\omega + s\omega'), \tag{44}$$

and

$$(a - b)\,\mu = \tfrac{1}{3}\left[(r - p)\,\omega + (s - q)\,\omega'\right], \tag{45}$$

$$\mu = \frac{(3m + r - p)\,\omega + (3m' + s - q)\,\omega'}{3(a - b)}, \tag{46}$$

$$\lambda = \frac{(3ma + ra - pb)\,\omega + (3m'a + sa - qb)\,\omega'}{3(a - b)}, \tag{47}$$

where each of the numbers m, m' has any value from 0 to $a - b - 1$ inclusive, from which it is evident that the number of such points (μ) is 1, $(a - b)$, or $(a - b)^2$, according as the curve is non-periodic, singly periodic, or doubly periodic, and the number of such points (λ) is $1, \frac{a-b}{\delta}$, or $\frac{(a-b)^2}{\delta^2}$, where δ is the greatest common divisor of a and b.

Formula (44) shows that, if $b = a$, then $r = p$ and $s = q$, as is evident from the fact that any $a_{r,s}$ is obtained from the $a_{p,q}$ by collineation first with a certain inflexion $0_{\rho(r-p),\rho(s-q)}$ and then with the inflexion 0_{00}, and the two points cannot coincide unless $0_{\rho(r-p),\rho(s-q)}$ coincides with 0_{00}, i. e. $r = p$ and $s = q$.

Equation (45) shows that if the $a_{p,q}$ of (μ) coincides with the $b_{r,s}$ of (μ), then

* Here and in the following pages I employ $\pm a$ to denote the absolute (positive) value of a.

the $(a-b)$ (with any suffices) of (μ) is a certain inflexion, and especially the $(a-b)_{\rho(p-r),\rho(q-s)}$ of (μ) is the inflexion 0_{00}.

Equation (42) enables us to determine the condition that of two points given by their parameters, one (λ) is a derivative of the other (μ). The condition is evidently that of the possibility of the determination of three integers a, p, q to satisfy the congruence (42). It will be convenient to consider λ under the form $\lambda_1\omega+\lambda_2\omega'$, and μ under the form $\mu_1\omega+\mu_2\omega'$, — a representation which is unambiguous if $\lambda_1, \lambda_2, \mu_1, \mu_2$ are real, since ω and ω' are respectively real and purely imaginary. The condition is then involved in these two:—

$$\left.\begin{aligned}\lambda_1 &\equiv a\mu_1+\tfrac{1}{3}p \,(\mathrm{mod.}\ 1),\\ \lambda_2 &\equiv a\mu_2+\tfrac{1}{3}q \,(\mathrm{mod.}\ 1),\end{aligned}\right\} \tag{48}$$

i. e. $\frac{1}{3}(3a\mu_1-3\lambda_1+p)$ and $\frac{1}{3}(3a\mu_2-3\lambda_2+q)$ are both integers, conditions which are certainly impossible unless λ_1 and μ_1, as also λ_2 and μ_2, are commensurable, in the sense that one can be expressed rationally in terms of the other and of absolute rationals; the most interesting case is that in which μ_1 and μ_2, and consequently λ_1 and λ_2, are rational quantities.

Periodic Points or Self-Derivatives.

A general problem which has many special forms of interest is this: to find a point (μ) whose $a_{p,q}$ coincides with it. The solution is given by

$$a\mu+\tfrac{1}{3}(p\omega+q\omega')\equiv\mu,$$

$$(a-1)\mu\equiv-\tfrac{1}{3}(p\omega+q\omega'),$$

$$\mu\equiv\frac{(3m-p)\,\omega+(3m'-q)\,\omega'}{3(a-1)}, \tag{49}$$

in which, to obtain all the different points (μ) for a given index $a_{p,q}$, to each of the integers m, m' must be given any $\pm(a-1)$ successive values. The number of such different points (μ) for the index $a_{p,q}$ is therefore 1, $\pm(a-1)$, or $(a-1)^2$, according as the cubic is non-periodic, singly periodic, or doubly periodic. On the non-periodic curve the only self-derivative is the inflexion, which corresponds to every index, and I therefore omit the further consideration of this case. Equation (49) may also be written

$$\mu\equiv\frac{(-3m+p)\,\omega+(-3m'+q)\,\omega'}{3[-(a-2)-1]}, \tag{50}$$

i. e. any self-$a_{p,q}$ is also a self-$[-(a-2)]_{\rho(-p),\rho(-q)}$, so that the indices go

together in pairs of *conjugates* (excepting the index $1_{0.0}$, which we need not consider, as every point is its own $1_{0.0}$) such that to each index of any pair of *complementary* indices, say, correspond the same self-derivatives. It is to be noticed that one of the indices of every pair is positive, so that the self-derivatives *may* be classed according to the positive index. However, in the formula (49) there occurs only $a - 1$, which has the same absolute value for any index a as for its conjugate. In what follows I therefore assume $a - 1$ to mean this absolute positive value, without writing the double sign, and take a either positive or negative.

If $3m - p$, $3m' - q$, and $a - 1$ in (49) have a common factor, the corresponding point (μ) may also be obtained for a less value of a (more exactly, for a less value of $a - 1$) with proper suffices. We may impose upon a, p, q any conditions we please (for instance, that a shall be of the form $3i + 1$, and $p = 0$, $q = 0$), which may be regarded as conditions imposed upon $3m - p$, $3m' - q$, and $a - 1$. Any point which is a self-derivative with the index $a_{p,q}$, but not a self-derivative with a less index, subject to the given conditions (say ψ) will be said to *belong to the index* $\mathrm{a}_{\mathrm{p},\mathrm{q}}$ (*conditions* ψ). The number of self-derivatives belonging to the index $a_{p,q}$ (conditions ψ) is evidently the number of pairs of numbers, the first of the form $3m - p$ and the second of the form $3m' - q$, neither greater than $3(a - 1)$, which do not *both* contain any divisor δ of $a - 1$ (other than 1) such that the quotients $\frac{3m - p}{\delta}$, $\frac{3m' - q}{\delta}$, and $\frac{a - 1}{\delta}$ also satisfy the given conditions. The pairs of values m, m' which are to be excluded are those which satisfy the congruences

$$3m \equiv p \,(\text{mod. } \delta) \qquad \text{and} \qquad 3m' \equiv q \,(\text{mod. } \delta),$$

where δ is some divisor of $a - 1$ satisfying a certain condition κ, which for convenience I assume to include the condition just stated that δ is a divisor of $a - 1$. With this proviso, κ is the condition that the quotients of $3m - p$, $3m' - q$, and $a - 1$, by δ, shall satisfy the conditions ψ.

If δ is not a multiple of 3, the number of numbers m not greater than $a - 1$ (subject to no condition) and satisfying the first of these congruences is $\frac{a-1}{\delta}$, which is also the number of numbers not greater than $a - 1$ and divisible by δ; and the number of values of m' satisfying the second congruence is the same. Hence, if $a - 1$ is not a multiple of 3, so that it has no divisor δ which is such a multiple, the number of numbers of the form $3m - p$, not greater than $3(a - 1)$, which have no divisor satisfying the condition κ, is $\overset{a-1}{\underset{1}{T}}[\mathrm{c}\,(\widehat{a - 1}) \,.\, \kappa]$,* and the

* See note at the end of this article for definitions of these *totients*.

number of pairs of numbers, the first of the form $3m-p$ and the second of the form $3m'-q$, neither greater than $3(a-1)$, which have no common divisor satisfying the condition κ, is $\overset{a-1}{\underset{1}{T}}\,[\breve{\bar{\mathrm{C}}}\,(\overset{\cdot}{\widehat{a-1}})\,.\,\kappa]^2$.

If δ is a multiple of 3, and p is not 0, there is no value of m which satisfies the congruence $3m \equiv p\,(\text{mod. }\delta)$. Hence, if $a-1$ has any divisors which are multiples of 3 satisfying the condition κ, and if p is 1 or 2, the number of numbers of the form $3m-p$, not greater than $3(a-1)$, which have no divisor satisfying the condition κ, is $\overset{a-1}{\underset{1}{T}}\,[\bar{\mathrm{C}}\,(\widehat{a-1})\,.\,\kappa\,.\,\bar{0}_3]$. Similarly, if $a-1$ has any divisors which are multiples of 3 satisfying the condition κ, and if either p or q (or both) is different from 0, the number of pairs of numbers, the first of form $3m-p$ and the second of the form $3m'-q$, neither greater than $3(a-1)$, which have no common divisor satisfying the condition κ, is $\overset{a-1}{\underset{1}{T}}\,[\breve{\bar{\mathrm{C}}}\,(\overset{\cdot}{\widehat{a-1}})\,.\,\kappa\,.\,\bar{0}_3]^2$.

If δ is a multiple of 3, and $p=0$, the number of numbers of the form $3m$, not greater than $3(a-1)$, which have in common with $a-1$ the divisor δ is $\frac{3(a-1)}{\delta}$, which is the number of numbers not greater than $a-1$ having in common with $a-1$ the divisor $\frac{1}{3}\delta$; in fact, if $3m$ contains δ, a multiple of 3, then m will contain $\frac{1}{3}\delta$, and conversely. The number of numbers of the form $3m$, not greater than $3(a-1)$, which have no divisor satisfying the condition κ, is $\overset{a-1}{\underset{1}{T}}\,[\bar{\mathrm{C}}\,(\widehat{a-1})\,.\,\kappa\,.\,(\bar{0}_3, \tfrac{1}{3}0_3)]$;* and the number of pairs of numbers, each of the form $3m$, neither greater than $3(a-1)$, which have no common factor satisfying the condition κ, is $\overset{a-1}{\underset{1}{T}}\,[\breve{\bar{\mathrm{C}}}\,(\overset{\cdot}{\widehat{a-1}})\,.\,\kappa\,.\,(\bar{0}_3, \tfrac{1}{3}0_3)]^2$.

From what precedes it is evident that the number of self-derivatives belonging to the index $a_{p,q}$ (conditions ψ) is given by the following table:—

		Singly Periodic Cubic.	Doubly Periodic Cubic.
a not of the form $3i+1$		$\overset{a-1}{\underset{1}{T}}[\bar{\mathrm{C}}\,(\widehat{a-1})\,.\,\kappa]$	$\overset{a-1}{\underset{1}{T}}[\breve{\bar{\mathrm{C}}}\,(\overset{\cdot}{\widehat{a-1}})\,.\,\kappa]^2$
a of the form $3i+1$	p and q not both 0	$\overset{a-1}{\underset{1}{T}}[\bar{\mathrm{C}}\,(\widehat{a-1})\,.\,\kappa\,.\,\bar{0}_3]$	$\overset{a-1}{\underset{1}{T}}[\breve{\bar{\mathrm{C}}}\,(\overset{\cdot}{\widehat{a-1}})\,.\,\kappa\,.\,\bar{0}_3]^2$
	p and q both 0	$\overset{a-1}{\underset{1}{T}}[\bar{\mathrm{C}}(\widehat{a-1}).\kappa.(\bar{0}_3, \tfrac{1}{3}0_3)]$	$\overset{a-1}{\underset{1}{T}}[\breve{\bar{\mathrm{C}}}(\overset{\cdot}{\widehat{a-1}})\,.\,\kappa\,.(\bar{0}_3, \tfrac{1}{3}0_3)]^2$

(51)

The number of *real* self-derivatives belonging to the index $a_{p,q}$ (conditions ψ) is found by taking into account the condition (41), which being applied to (49) gives

$$2(3m'-q) \equiv 0\ [\text{mod. } 3(a-1)].$$

* For convenience, I have used here $\bar{\mathrm{C}}\,(\widehat{a-1})\,.\,\kappa\,.\,\tfrac{1}{3}0_3$ to denote "does not contain one third of any divisor of $a-1$ of the form $3i$ which satisfies the condition κ."

Now $3m' - q$ is never greater than $3(a-1)$; hence the only values of m' which will correspond to real points are those for which

$$3m' - q = 3(a-1) \text{ or the congruent value } 0, \text{ and } 3m' - q = \tfrac{3}{2}(a-1),$$

neither of which can be satisfied unless $q = 0$; and if $q = 0$, the solutions are, respectively, $m' = a - 1$ or 0, and $m' = \frac{1}{2}(a-1)$, which latter solution exists only when a is odd. Hence, whatever the given conditions, no *real* self-derivative belongs to any index of the type $a_{p,1}$ or $a_{p,2}$; and to the index $a_{p,0}$ belong both or only the first of the self-derivatives

$$\mu = \frac{3m - p}{3(a-1)}\,\omega \qquad \text{and} \qquad \mu = \frac{3m-p}{3(a-1)}\,\omega + \tfrac{1}{2}\omega', \tag{52}$$

according as a is odd or even, in each of which all values not greater than $a - 1$ (or any natural succession of $a-1$ values) are to be assigned to m, rejecting only those for which $3m - p$ has in common with $a-1$ a factor satisfying the conditions κ. The number of *real* self-derivatives on a doubly periodic cubic is then, by (51):—

$$\begin{array}{lll}
\mathop{T'}\limits_{1}^{a-1}[\bar{c}(\widehat{a-1}).\kappa] & \text{if } a \text{ is of the form} & 6i \text{ or } 6i+2, \\
2\mathop{T}\limits_{1}^{a-1}[\bar{c}(\widehat{a-1}).\kappa] & \text{"} \quad \text{"} & 6i+3 \text{ or } 6i+5, \\
2\mathop{T}\limits_{1}^{a-1}[\bar{c}(\widehat{a-1}).\kappa.\bar{0}_3] & \text{"} \quad \text{"} & 6i+1 \text{ and } p \text{ is } 1 \text{ or } 2, \\
\mathop{T}\limits_{1}^{a-1}[\bar{c}(\widehat{a-1}).\kappa.\bar{0}_3] & \text{"} \quad \text{"} & 6i+4 \text{ and } p \text{ is } 1 \text{ or } 2, \\
2\mathop{T}\limits_{1}^{a-1}[\bar{c}(\widehat{a-1}).\kappa.(\bar{0}_3, \tfrac{1}{3}0_3)] & \text{"} \quad \text{"} & 6i+1 \text{ and } p \text{ is } 0, \\
\mathop{T}\limits_{1}^{a-1}[\bar{c}(\widehat{a-1}).\kappa.(\bar{0}_3, \tfrac{1}{3}0_3)] & \text{"} \quad \text{"} & 6i+4 \text{ and } p \text{ is } 0;
\end{array} \tag{53}$$

i. e. the number of *real* self-derivatives (suffices p, q) on a doubly periodic cubic is the same as or double the number of self-derivatives (suffices p, q) on a singly periodic cubic, according as a is even or odd.

On a singly periodic cubic with real period only the first of equations (52) is to be employed, and all the self-derivatives are real. The only real self-derivatives on a singly periodic cubic with imaginary period are those points for which

$$\mu = 0 \qquad \text{and} \qquad \mu = \tfrac{1}{2}\omega',$$

the former of which corresponds (in an improper sense) to every index, and the latter (in the same sense) to every odd index; the latter is the point of contact

of the tangent which can be drawn from the real inflexion to touch the curve elsewhere.

If no conditions ψ are given, I say simply that the self-derivative (μ) *belongs to* the index $a_{p,q}$. If to m be assigned successively all values not exceeding $a-1$, and to p each of the values 2, 1, 0, the number $3m-p$ assumes successively all values not exceeding $3(a-1)$, and each value but once. Hence the number of self-derivatives belonging to the index $a_{p,q}$ is the number of pairs of numbers, the first of the form $3m-p$ and the second of the form $3m'-q$, neither greater than $3(a-1)$, which have no common divisor which divides also $a-1$; and this number is found from (51) by making the condition κ mean only "divisor of $a-1$," i. e. in the notation of the appended note

$$\kappa = (\widehat{a-1}). \tag{54}$$

In this classification, if a is of the form $3i+1$ and p and q are both 0, since there is no condition imposed upon the least divisors of $a-1$, the only least divisor which is a 0_3 is 3 itself; hence

$$\overset{a-1}{\underset{1}{T}}[\bar{\text{O}}\,\kappa\,.\,(\bar{0}_3\,,\tfrac{1}{3}\,0_3)] = \overset{a-1}{\underset{1}{T}}[\bar{\text{O}}\,\kappa\,.\,(\bar{0}_3\,,1)] = 0,$$

because it contains the vanishing factor $\left(1-\frac{1}{1}\right)$. Hence no self-derivative belongs to the index $a_{0,0}$, if a is of the form $3i+1$, and no condition is imposed. These results apply to the doubly periodic cubic; for the singly periodic cubic, the number of self-derivatives belonging to the index $a_{p,0}$ or $a_{0,q}$, according as the period is real or imaginary, is the number of numbers of the form $3m-p$ or $3m'-q$, not greater than $a-1$, which have no common divisor which divides $a-1$; and this number is also found from (51) by determining κ to satisfy (54) alone.

The first classification of self-derivatives under an imposed condition which I shall consider is that in which the suffices are given; thus, in accordance with the above convention, I shall speak of the self-derivatives belonging to the index a (suffices p, q); it is needless in this case to repeat the suffices. As an example of this kind of classification consider the point corresponding to $\mu = \frac{5}{6}\,\omega + \frac{2}{3}\,\omega'$, which may be written

$$\mu = \frac{(3\,.\,2-1)\,\omega + (3\,.\,2-2)\,\omega'}{3\,(3-1)} = \frac{(3\,.\,4-2)\,\omega + (3\,.\,3-1)\,\omega'}{3\,(5-1)} = \frac{3\,.\,5\,\omega + 3\,.\,4\,\omega'}{3\,(7-1)},$$

which belongs to the indices $3_{1,2}$ and $-1_{2,1}$ (no conditions); but in the present classification it belongs to the indices 3 and -3 (suffices 1, 2), to 5 and -1

(suffices 2, 1), and to 7 and -5 (suffices 00). The condition ψ that a self-derivative given by (49) shall belong to the index a (suffices p, q) is evidently that $3m - p$, $3m' - q$, and $a - 1$ shall contain no common factor δ such that $3m - p$ and $3m' - q$ shall have, respectively, the same residues (mod. 3) as their quotients by δ. This constancy of residue is the condition κ. If p and q are not both 0, this condition is satisfied when δ is of the form $3i + 1$, and only then, so that $\kappa = \widehat{(a-1)}\,.\,1_3$; but if p and q are both 0, $\frac{3m}{\delta}$ will contain 3 when m contains δ, i.e. the condition ψ will be satisfied if m is a divisor of $a - 1$; so that $\kappa = \widehat{(a-1)}$.

In this classification, therefore, the number of self-derivatives belonging to the index a (suffices p, q) is as follows:—

p and q.	Singly Periodic with Real Period.	Doubly Periodic.
Not both 0	$\overset{a-1}{\underset{1}{T}}[\bar{\mathrm{C}}\,\widehat{(a-1)}\,.\,1_3]$	$\overset{a-1}{\underset{1}{T}}[\breve{\bar{\mathrm{C}}}\,\widehat{(a\dot{-}1)}\,.\,1_3]^2$
Both 0	$\tau\,(a-1)$	$\tau^2\,(a-1)$

(55)

A very important classification of self-derivatives is that according to the least index having a given residue (mod. 3) with given suffices, say ($\equiv a$, mod. 3; suffices p, q). It is evident that, unless a is of the form $3i + 1$, and p and q are both 0, the number of self-derivatives belonging to the index a ($\equiv a$, mod. 3; suffices p, q) is $\overset{a-1}{\underset{1}{T}}[\bar{\mathrm{C}}\,\widehat{(a-1)}\,.\,1_3]$ or $\overset{a-1}{\underset{1}{T}}[\breve{\bar{\mathrm{C}}}\,\widehat{(a\dot{-}1)}\,.\,1_3]^2$, according as the cubic is singly or doubly periodic. If a is of the form $3i + 1$, and p and q are both 0, the condition κ is that the divisor δ shall be such that the quotients $\frac{3m}{\delta}$, $\frac{3m'}{\delta}$, $\frac{a-1}{\delta}$ are all multiples of 3, as the first two are if δ is a divisor of m and m', and $\frac{a-1}{\delta}$ will be if 3 occurs as a factor to a higher power in $a - 1$ than in δ; if $a - 1$ contains 3 to a higher power than the first, every factor of $a - 1$ will have a divisor δ containing 3 to a less power than occurs in $a - 1$; but if $a - 1$ contains only the first power of 3, then every factor of $a - 1$, excepting only 3 itself, will have a divisor δ which contains 3 to a less power than occurs in $a - 1$, but 3 will not have such a divisor. Hence, if a is of the form $9i + 1$, and p and q are both 0, the number of self-derivatives belonging to a ($\equiv 1$, mod. 3; suffices 00) is $\tau\,(a - 1)$ for a singly periodic, and $\tau^2\,(a - 1)$ for a doubly periodic cubic; and if a is of the form $3i + 1$ but not of the form $9i + 1$, and p and q are both 0, the number of self-derivatives belonging to

a ($\equiv 1$, mod. 3; suffices 00) is $\overset{a-1}{\underset{1}{T}}[\bar{c}(\widehat{a-1}).\bar{0}_3]$ for a singly periodic, and $\overset{a-1}{\underset{1}{T}}[\breve{\bar{c}}(\widehat{\dot{a}-1}).\bar{0}_3]^2$ for a doubly periodic cubic.

If p and q are both 0, and a is of the form $3i+1$ or $-3i+1$,* where i is a positive integer, the self-derivatives are *pertactile* points of the grade i (Sylvester, page 74). The condition that a point (μ) should be a pertactile point belonging to the grade i is

$$\mu = \frac{m\omega + m'\omega'}{3i}, \tag{56}$$

where neither m nor m' exceeds $3i$, and m, m', and i have no common divisor. If i is a multiple of 3, $3i$ contains no prime factors which i does not, and the number of such points is $\tau(3i)$ or $\tau^2(3i)$, according as the cubic is singly or doubly periodic. If i is not a multiple of 3, $3i$ contains one prime factor, viz. 3, which i does not, and hence those numbers m and m', which contain only the factor 3 in common with $3i$, do not correspond to pertactile points of lower grade, and the number of pertactile points belonging to the grade i is $\overset{3i}{\underset{1}{T}}[\bar{c}(\widehat{3i}).\bar{0}_3]$ or $\overset{3i}{\underset{1}{T}}[\breve{\bar{c}}(\widehat{3i}).\bar{0}_3]^2$, according as the cubic is singly or doubly periodic. From the values of these totients given in the appended note, it is easy to see that, whatever the value of i, the number of pertactile points belonging to the grade i is $3\tau(i)$ or $9\tau^2(i)$, according as the cubic is singly or doubly periodic, which last result agrees with that given by Professor Sylvester (page 76).

In general, if (μ) is a self-derivative belonging (conditions given) to the index $a_{p,q}$, it follows from (49) that

$$\begin{aligned}
(a-1)\mu &\equiv -\tfrac{1}{3}(p\omega+q\omega'), & -(a-1)\mu &\equiv \tfrac{1}{3}(p\omega+q\omega'),\\
a\mu &\equiv \mu - \tfrac{1}{3}(p\omega+q\omega'), & -a\mu &\equiv -\mu + \tfrac{1}{3}(p\omega+q\omega'),\\
(a-2)\mu &\equiv -\mu - \tfrac{1}{3}(p\omega+q\omega'), & -(a-2)\mu &\equiv \mu + \tfrac{1}{3}(p\omega+q\omega').
\end{aligned} \tag{57}$$

Now, according as a is of the form $3i+1$, $-3i+1$, $3i-1$, $-3i$, $3i$, or $-3i-1$, where i is a positive integer, the number $-(a-2)$, a, $-a$, $a-2$, $-(a-1)$, or $a-1$ is of the form $-3n+1$, where n is a positive integer, viz. $n=i$ unless a is of the form $-3i$ or $-3i-1$, and then $n=i+1$. That is, in the six cases, respectively,

---

* As has been remarked in connection with (50), the self-derivatives belonging to the index $a_{p,q}$ belong also to the index $-(a-2)_{\rho(p),\rho(q)}$, so that the indices go together in pairs, thus: $3i+1$, $-3i+1$; $3i$, $-3i+2$; $3i+2$, $-3i$ are the forms of pairs of indices to which belong the same self-derivatives, and in the following I shall assume such a grouping without further mention. Especially is this grouping useful when p and q are both 0, for $\rho(0)=0$, so that the suffices of any index (suffices 00) are the same as of the complementary index.

$$(-3n+1)\,\mu \equiv \mu + \tfrac{1}{3}(p\omega + q\omega'),\ \mu - \tfrac{1}{3}(p\omega + q\omega'),\ -\mu + \tfrac{1}{3}(p\omega + q\omega'),$$
$$-\mu - \tfrac{1}{3}(p\omega + q\omega'),\ \tfrac{1}{3}(p\omega + q\omega'),\ -\tfrac{1}{3}(p\omega + q\omega'),$$

so that, if a curve of the order n be passed through $3n-1$ consecutive points on the cubic at (μ), i. e. have $(3n-1)$-point* contact with the cubic at (μ), the $(3n)^{\text{th}}$ intersection of such a curve with the cubic will be, in the six cases respectively, the $1_{p,q}$, $1_{\rho(p),\rho(q)}$, $-1_{p,q}$, $-1_{\rho(p),\rho(q)}$, $0_{p,q}$, $0_{\rho(p),\rho(q)}$ of (μ); in the first two cases, if p and q are both 0, the $(3n)^{\text{th}}$ intersection will be the point (μ) itself, and in the last two cases it is a constant point, viz. an inflexion. These latter cases appear as special forms of the problem: to determine the points (μ) at which a curve of the order n passing through a given point (λ) of the cubic may have $(3n-1)$-point contact, the solution of which is given by $-(3n-1)\,\mu = \lambda$, so that (μ) is a sub-$(-3n+1)_{00}$ of (λ).

To the subject of self-derivatives belongs the problem of the in- and exscribed k-laterals, which may be stated thus: to construct a polygon of k sides, each tangent to the cubic at its intersection with the preceding side; or, in other words, to determine a point on the cubic, whose k^{th} tangential coincides with it. It is evident that the index of the k^{th} tangential of 1_{00}, which is found by a repetition of formula (2), is $(-2)^k_{00}$; hence the condition that (μ) shall be a vertex of an in- and exscribed k-lateral is $(-2)^k\mu \equiv \mu$, i. e. $2^k\mu \equiv (-1)^k\mu$, or

$$\mu \equiv \frac{m\omega + m'\omega'}{2^k - (-1)^k}, \tag{58}$$

where m and m' have any values not exceeding $2^k - (-1)^k$; the number $\psi(k)$ of vertices of *proper* k-*laterals*, i. e. corresponding to k but to no divisor of k, is

$$\overset{2^k-(-1)^k}{\underset{1}{T}}\left[\breve{\text{c}}\left(2^k-(-1)^k\right).\kappa\right] \quad \text{or} \quad \overset{2^k-(-1)^k}{\underset{1}{T}}\left[\breve{\text{c}}\left(2^k-(-1)^k\right).\kappa\right]^2,$$

for a singly or doubly periodic cubic respectively, where the condition κ is to be taken to mean that the quotient of $2^k - (-1)^k$ by the divisor, is still of the form $2^i - (-1)^i$. Now $2^i - (-1)^i$ is a divisor of $2^k - (-1)^k$ if i is a divisor of k, and only then. For a singly periodic cubic, then, if $1, d, d', \ldots., k$ are the different divisors of k,

$$\psi(1) + \psi(d) + \psi(d') + \ldots. + \psi(k) = 2^k - (-1)^k; \tag{59}$$

therefore, if $\alpha, \beta, \gamma, \ldots.$ are the different prime factors of k, and if for convenience $2^k - (-1)^k$ is represented by $f(k)$,

---

* I make a distinction between k-point contact and k-tuple contact of two curves, the former implying k, and the latter $k+1$ consecutive common points, although I believe such a distinction is not usual.

$$\psi(k) = f(k) - \Sigma' f\left(\frac{k}{\alpha}\right) + \Sigma'' f\left(\frac{k}{\alpha\beta}\right) - \Sigma''' f\left(\frac{k}{\alpha\beta\gamma}\right) + \ldots, \qquad (60)$$

where Σ', Σ'', Σ''', ... denote summation with respect to all the factors α, β, γ, ..., their binary, ternary, etc., products (for a proof of the theorem that (59) implies (60), see Dirichlet's *Zahlentheorie*, edited by Dedekind, § 138, or Bachmann's *Kreistheilung*, pp. 8–11); in other words,*

$$\psi(k) = [2^{()} - (-1)^{()}]\, \tau(k) = [2^{()}]\, \tau(k). \qquad (61)$$

The equality of the second and third members of this equation follows from the fact that, in the prime totient of k, according to which the sum is taken in (61), the number of positive even terms is the same as that of negative even terms, and the number of positive odd terms is the same as that of negative odd terms,† so that

$$[(-1)^{()}]\, \tau(k) = 0.$$

If the cubic is doubly periodic, (59) is to be replaced by

$$\psi(1) + \psi(d) + \psi(d') + \ldots + \psi(k) = \left(2^k - (-1)^k\right)^2, \qquad (62)$$

and hence follows, by virtue of the theorem above cited,

$$\psi(k) = f^2(k) - \Sigma' f^2\left(\frac{k}{\alpha}\right) + \Sigma'' f^2\left(\frac{k}{\alpha\beta}\right) - \Sigma''' f^2\left(\frac{k}{\alpha\beta\gamma}\right) + \ldots, \qquad (63)$$

where $f^2(k)$, ..., are the squares of $f(k)$, ..., i.e.

$$\psi(k) = [2^{()} - (-1)^{()}]^2\, \tau(k) = [(-2)^{2()} - 2(-2)^{()}]\, \tau(k). \qquad (64)$$

From (58) it is evident that $k = 1$ gives all the inflexions, which are also *improper* solutions for every value of k, since $2^k - (-1)^k$ is divisible by 3, whatever value k may have.

Since $2^k - (-1)^k$ is necessarily odd, and hence $\frac{1}{2}[2^k - (-1)^k]$ cannot be an integer, it follows from a comparison of (58) and (41) that the number of *real*

---

* See "Note on Totients" at the end of this paper.

† Namely, let n be the number of different prime factors of k. If k is odd, all its prime factors are odd, and all the terms of its prime totient are odd, 2^{n-1} of them being positive, and 2^{n-1} negative. If k is oddly even, i.e. contains 2 but not 4, one of the prime factors of k is 2, and its prime totient contains the factor $(2-1)$, and otherwise only odd factors (i.e. odd monomial factors and binomial factors of the form $a - 1$, where a is odd), so that 2^{n-2} terms are positive and even, 2^{n-2} negative and even, 2^{n-2} positive and odd, 2^{n-2} negative and odd. If k is evenly even, i.e. contains 4, its prime totient contains the factor 2, and every term is even, 2^{n-1} being positive, and 2^{n-1} negative. If $k = 1$, $\tau(k) = 1$, and $[2^{()} - (-1)^{()}]\, \tau(1) = 3$; and if $k = 2$, $\tau(k) = 2 - 1$, $[2^{()} - (-1)^{()}]\, \tau(2) = 0$; which are the only exceptions.

vertices of proper k-laterals in- and exscribable to a singly periodic cubic with real period or a doubly periodic cubic is $[2^{()}]\,\tau(k)$, but that there are no such real vertices on a non-periodic cubic or a singly periodic cubic with imaginary period, excepting the one real inflexion on each of the latter cubics. The number of proper k-laterals in- and exscribable to a cubic is then given by the following table (excluding inflexions).

Species of Cubic.	Real and Imaginary.	Real.
CUSPIDAL (non-periodic)	0	0
CRUNODAL (singly periodic with imaginary period)	$\frac{1}{k}[2^{()}]\,\tau(k)$*	0
ACNODAL (singly periodic with real period)	$\frac{1}{k}[2^{()}]\,\tau(k)$	$\frac{1}{k}[2^{()}]\,\tau(k)$
NON-SINGULAR (doubly periodic)	$\frac{1}{k}[(-2)^{2()}-2(-2)^{()}]\,\tau(k)$	$\frac{1}{k}[2^{()}]\,\tau(k)$†

(65)

As Professor Sylvester has remarked,‡ the number of proper k-laterals in- and exscribable to a non-singular cubic shows that $[2^{()}-(-1)^{()}]^2\,\tau(k)$ is always divisible by k; but the method here employed shows that, if a is any integer whatever, positive or negative, every point (μ) for which a^k of (μ) coincides with (μ) is given by

$$\mu=\frac{m\omega+m'\omega'}{a^k-1}; \tag{66}$$

hence, by the same reasoning as above,

$$[a^{()}-1]\,\tau(k)=[a^{()}]\,\tau(k)$$

and

$$[a^{()}-1]^2\,\tau(k)=[a^{2()}-2\,a^{()}]\,\tau(k)$$

are divisible by k; in general, $[a^{()}-1]^i\,\tau(k)$, where i is any positive integer, is

* Compare Rosenow, *Die Curven dritter Ordnung mit einem Doppelpunkte*, p. 41, and Durège, *Ueber fortgesetztes Tangentenziehen an Curven dritter Ordnung mit einem Doppel- oder Rückkehrpunkte*, Math. Annalen, Vol. I.

† Compare Harnack, *Ueber die Verwerthung der elliptischen Functionen für die Geometrie der Curven dritten Grades*, Math. Annalen, Vol. IX. p. 12, footnote.

‡ This Journal, Vol. II. p. 386.

also divisible by k, for it may be developed as a sum of terms of the form $C\,.\,[a^{(\,)}]^r\,\tau(k)$ (where C and r are integers, of which the latter is positive), each of which terms contains k. Thus, not only the last member of (64), but each of its terms, is divisible by k.

On page 75 Professor Sylvester has obtained a result which may be more explicitly stated thus: If any $(3a)_{p,q}$ of (λ) coincides with the inflexion $0_{p,q}$, then the $a_{r,s}$ of (λ) will coincide with some inflexion; namely, the $a_{r,s}$ of a^2 different sub-$(3a)_{p,q}$'s of (λ) will coincide with any given inflexion, r and s being given, and the $a_{r,s}$ of any given sub-$(3a)_{p,q}$ of (λ) will coincide with any given inflexion for some *one* set of values of r and s. We may solve, by the preceding methods, this more general problem: —

If the $(ab)_{p,q}$ of (λ) is a given inflexion, under what conditions will the $a_{r,s}$ of (λ) also be an inflexion, and what inflexion will it be?

Let the given inflexion be $\frac{1}{3}(\mu\omega + \mu'\omega')$, then

$$\lambda = \frac{(\mu - p + 3m)\,\omega + (\mu' - q + 3m')\,\omega'}{3ab}, \tag{67}$$

where each of the numbers m and m' has any ab successive values, and the

$$a_{r,s} \text{ of } (\lambda) = \frac{(\mu - p + 3m + br)\,\omega + (\mu' - q + 3m' + bs)\,\omega'}{3b}, \tag{68}$$

which is an inflexion if

$$\mu - p + 3m \equiv 0 \quad \text{and} \quad \mu' - q + 3m' \equiv 0 \pmod{b},$$

and only then. If then b is not a multiple of 3, the values of m and m' satisfying these conditions will be found from

$$3m \equiv p - \mu \quad \text{and} \quad 3m' \equiv q - \mu' \pmod{b}, \tag{69}$$

and the number of points (λ) found by substituting these values in the above expression for λ is a^2; but if b is a multiple of 3, the congruences for m and m' have solutions only when $\mu - p$ and $\mu' - q$ are also divisible by 3, i.e. (since each of the numbers μ, μ', p, q has the value 0, 1, or 2) only when $\mu = p$ and $\mu' = q$; and if these conditions are satisfied, then

$$m \equiv 0 \quad \text{and} \quad m' \equiv 0 \pmod{\tfrac{1}{3}b}, \tag{70}$$

which give $9a^2$ points (λ) satisfying the given conditions. In either case say $3m = p - \mu + tb$, $3m' = q - \mu' + ub$, then

$$a_{r,s} \text{ of } (\lambda) = \frac{(r + t)\,\omega + (s + u)\,\omega'}{3}, \tag{71}$$

which may be *any* inflexion depending on the values of t and u. If $b=3$, $\mu=p$, $\mu'=q$, equations (70) show that m and m' may be any integers; this is the special case to which reference has been made above.

Note on Totients.

In the foregoing paper reference has been made to certain numbers called "totients." A *totient* is the number of things which satisfy certain conditions. These conditions may be of any nature, affirmative or negative. The things satisfying the prescribed conditions are called *totitive* to that condition, or simply *totitives.* Every science has its totitives, whose nature depends upon the subject matter of the science, and the determination of the totient or number of things satisfying any possible conditions constitutes a distinct branch of the science, which may itself be designated as the *totics* of the subject. For instance, we have *geometrical totics* (German, "Abzählende Geometrie"), the province of which is to determine the number of geometrical figures or curves satisfying certain conditions. I propose here to give an outline of a notation for *arithmetical* totients, and some formulæ belonging to *arithmetical totics.*

I use the following notation:—

$a, b, c, d, n, p, q, \alpha, \beta, \gamma$, denote integers.

κ, χ, are logical symbols denoting conditions satisfied.

r_d (read "an r to d") is a logical symbol denoting that division by d leaves the remainder r.

$\hat{a}$ denotes some (or any) divisor of a (other than 1).

c denotes "contains as divisor," and is followed by the number contained.

Besides the usual arithmetical multiplication and addition, it is necessary in combining *conditions* to employ logical multiplication and addition, which I denote by (.) and (,) respectively, with these definitions:—

$\kappa\,.\,\chi$ denotes that κ and χ are both (separately) satisfied.

$\kappa\,,\,\chi$ denotes that either κ or else χ is satisfied.

The logical product of two or more *numbers* denotes their least common multiple.

Whenever it becomes necessary to indicate how far the force of a logical sign or symbol extends, I use parentheses in conformity with the usual convention in the case of the arithmetical signs. With respect to the symbol c or $\bar{\mathsf{c}}$, it is assumed that the force of each extends over the signs (.) and (,). A dash over any logical symbol indicates that the condition denoted by that symbol is not satisfied; thus, $\bar{r}_d$ denotes that division by d leaves a remainder different from r.

$\overline{\kappa\, ,\, \chi}$ indicates that neither κ nor χ is satisfied.

$\overline{\kappa\, .\, \chi}$, that κ and χ are not both satisfied.

$\mathsf{c}\hat{n}$ denotes "contains some factor of n," and $\bar{\mathsf{c}}\hat{n}$ "contains no factor of n."

A condition, or logical product or sum of conditions standing by itself denotes any number satisfying the simple or compound condition.

$\overset{q}{\underset{p}{T}}[\kappa]$ denotes the totient to the condition κ within the limits p to q, i. e. the number of numbers from p to q, inclusive, which satisfy the condition κ.

$T[\overset{q}{\underset{p}{\kappa}}]\,[\overset{s}{\underset{r}{\chi}}]$ denotes the number of pairs of numbers, the first between p and q, inclusive, satisfying the condition κ, and the second between r and s, inclusive, satisfying the condition χ.

$\overset{q}{\underset{p}{T}}[\kappa]^k$ denotes the number of sets of k numbers, each satisfying the condition κ, and between p and q, inclusive, counting repetitions due to different permutations of the numbers of any set. This notation may be extended indefinitely.

It is evident that

$$T[\overset{q}{\underset{p}{\kappa}}]\,[\overset{s}{\underset{r}{\chi}}] = \overset{q}{\underset{p}{T}}[\kappa]\,\overset{s}{\underset{r}{T}}[\chi],$$

and

$$\overset{q}{\underset{p}{T}}[\kappa]^k = (\overset{q}{\underset{p}{T}}[\kappa])^k,$$

whenever κ is a self-existent condition, i. e. one which may be predicated or denied of each number in the set of k, without reference to any other. For example, the condition $\bar{\mathsf{c}}\hat{n}$ is self-existent, but $\bar{\mathsf{c}}\hat{n}$ is not.

Similarly $\overset{q}{\underset{p}{T}}[\bar{\kappa}]$ is the number of numbers within the limits p to q, which do not satisfy the condition κ.

In the case of totients corresponding to *sets of numbers* it may be necessary to express conditions which are imposed upon each number of the set, but not independently of the other numbers. For this purpose I use the following notation:—

$[\kappa]^k$ denotes a set of k numbers *each* satisfying the condition κ.

$[\bar{\kappa}]^k$ denotes a set of k numbers *neither* satisfying the condition κ.

$[\breve{\kappa}]^k$ denotes a set of k numbers *some* (at least one) satisfying the condition κ.

$[\overset{\smile}{\bar{\kappa}}]^k$ denotes a set of k numbers *not all* (some not) satisfying the condition κ.*

* The notations $\breve{\kappa}$ and $\overset{\smile}{\bar{\kappa}}$ are borrowed from Mr. Peirce's *Algebra of Logic*, this volume, page 22.

$\hat{a}$ denotes some (any) factor of a, the same for each number of the set in question (usually to be read "any common factor of a"). For $k = 1$, $[\kappa]$ and $[\breve{\kappa}]$ are identical, as are also $[\bar{\kappa}]$ and $[\breve{\bar{\kappa}}]$.

In general,

$$\overset{n}{\underset{1}{T}}[\kappa] + \overset{n}{\underset{1}{T}}[\bar{\kappa}] = n, \qquad \overset{n}{\underset{1}{T}}[\kappa]^k + \overset{n}{\underset{1}{T}}[\breve{\bar{\kappa}}]^k = n^k, \qquad \overset{n}{\underset{1}{T}}[\bar{\kappa}]^k + \overset{n}{\underset{1}{T}}[\breve{\kappa}]^k = n^k. \tag{72}$$

According to the notation just explained, $\overset{n}{\underset{1}{T}}[\bar{\mathrm{c}}\hat{n}]$ denotes the number of numbers not greater than n and relatively prime to it; it may be called the *prime totient* of n, and represented, for the sake of brevity, by $\tau(n)$, a notation introduced by Professor Sylvester to replace the customary $\phi(n)$. Similarly $\overset{n}{\underset{1}{T}}[\breve{\bar{\mathrm{c}}}\hat{n}]^k$, the number of sets of k numbers, neither greater than n, which do not *all* contain any one factor of n, may be called the k^{th} *prime* totient of n, and represented by $\tau^k(n)$; Professor Sylvester has called $\tau^2(n)$ the "quadritotient" of n.

The totients which I have had occasion to use in the foregoing paper are those expressing the number of numbers within certain limits which have no divisors in common with a given number n, which satisfy certain conditions, i. e. totients of the type

$$\overset{n}{\underset{1}{T}}[\bar{\mathrm{c}}\hat{n} \,.\, \kappa], \qquad \overset{n}{\underset{1}{T}}[\breve{\bar{\mathrm{c}}}\hat{n} \,.\, \kappa]^k.$$

In what follows I assume:—

$a, b, c, \ldots.,$ to be all the different *prime* factors of n, so that $n = a^\alpha b^\beta c^\gamma, \ldots.;$

$1, d, d', \ldots., n$ to be all the different divisors of n; and

$\delta, \delta', \delta'', \ldots.,$ to be a complete system of *least* divisors of n satisfying the condition κ. By a system of *least divisors* I mean a system of divisors of which no one is a multiple of any other. Then, evidently,

$$\overset{n}{\underset{1}{T}}[\mathrm{c}d] = n\,\frac{1}{d}, \qquad \overset{n}{\underset{1}{T}}[\mathrm{c}\dot{d}]^k = n^k\,\frac{1}{d_k}, \tag{73}$$

$$\overset{n}{\underset{1}{T}}[\mathrm{c}d \,.\, d'] = n\,\frac{1}{d \,.\, d'}, \qquad \overset{n}{\underset{1}{T}}[\mathrm{c}d \,.\, d']^k = n^k\,\frac{1}{d^k\ d'^k}, \tag{74}$$

and hence follows, by (72),

$$\overset{n}{\underset{1}{T}}[\bar{\mathrm{c}}d] = n\,(1 - \tfrac{1}{d}), \qquad \overset{n}{\underset{1}{T}}[\breve{\bar{\mathrm{c}}}d]^k = n^k\left(1 - \frac{1}{d^k}\right). \tag{75}$$

The repetition of these formulæ gives

$$\begin{aligned} \tau(n) &= \overset{n}{\underset{1}{T}}[\mathrm{c}\hat{n}] = n\left(1 - \frac{1}{a}\right)\left(1 - \frac{1}{b}\right)\left(1 - \frac{1}{c}\right)\ldots., \\ \tau^k(n) &= \overset{n}{\underset{1}{T}}[\breve{\bar{\mathrm{c}}}\hat{n}] = n^k\left(1 - \frac{1}{a^k}\right)\left(1 - \frac{1}{b^k}\right)\left(1 - \frac{1}{c^k}\right)\ldots., \end{aligned} \tag{76}$$

of which the first is given in all the text-books, and the second, for the particular case $k = 2$, is given by Professor Sylvester (page 76).

The same method gives also

$$\begin{aligned} \overset{n}{\underset{1}{T}}[\mathrm{c}\hat{n}\,.\,\kappa] &= n\left(1-\tfrac{1}{\delta.}\right)\left(1-\tfrac{1}{\delta'.}\right)\left(1-\tfrac{1}{\delta''.}\right)\ldots\ldots, \\ \overset{n}{\underset{1}{T}}[\breve{\mathrm{c}}\hat{n}\,.\,\kappa] &= n^k\left(1-\tfrac{1}{\delta^k_{\cdot}}\right)\left(1-\tfrac{1}{\delta'^k_{\cdot}}\right)\left(1-\tfrac{1}{\delta''^k_{\cdot}}\right)\ldots\ldots, \end{aligned} \tag{77}$$

in which, as is indicated by the dots, the products of factors δ, δ', δ'', ..., in the denominators of the expanded expressions are *logical* products, i. e the *least common multiples* of their factors. More generally, if δ, δ', δ'', ... is the complete system of least divisors of n for the condition κ, and δ_1, δ_1', δ_1'', ..., the complete system for the condition χ,

$$\begin{aligned} \overset{n}{\underset{1}{T}}[\mathrm{c}(\hat{n}\,.\,\kappa)\,.\,\mathrm{c}(\hat{n}\,.\,\chi)] &= n\left(1-\tfrac{1}{\delta.}\right)\left(1-\tfrac{1}{\delta'.}\right)\left(1-\tfrac{1}{\delta''.}\right)\ldots\ldots\frac{1}{\delta_1\cdot}\,\frac{1}{\delta_1'\cdot}\,\frac{1}{\delta_1''\cdot}\ldots\ldots, \\ \overset{n}{\underset{1}{T}}[\breve{\mathrm{c}}(\hat{n}\,.\,\kappa)\,.\,\mathrm{c}(\hat{n}\,.\,\chi)]^k &= n^k\left(1-\tfrac{1}{\delta.^k}\right)\left(1-\tfrac{1}{\delta'.^k}\right)\left(1-\tfrac{1}{\delta''.^k}\right)\ldots\ldots\frac{1}{\delta^k_1.}\,\frac{1}{\delta_1'.^k}\,\frac{1}{\delta_1''.^k}\ldots\ldots, \end{aligned} \tag{78}$$

where $\hat{n}$ does not necessarily denote the same divisor of n under the sign c as under the sign $\breve{\mathrm{c}}$.*

The condition κ in (77) and (78) is that which expresses any *bonâ fide* property or properties of the divisor, e. g. that the divisor be the sum of two squares, or that it be $\equiv 2 \pmod{5}$. It cannot in general be a property of the quotient of n by the divisor. However, if ψ be a given property, there will, in general, be a condition κ to which, if d be subjected, the quotient of n by d will have the property ψ, as has been assumed above in (51) and (53). The following is an example of this mutual implication: the number of pairs of numbers ν, neither greater than n, and not *both* containing any divisor d of n, such that the quotient $\frac{n}{d}$ is of the form r_3, may be denoted by $\overset{n}{\underset{1}{T}}\left[\breve{\mathrm{c}}(d=\hat{n})\,.\left(\frac{n}{d}=r_3\right)\right]^2$, and is given by the following table:—

* It may be remarked that, provided all the *least* divisors for the various conditions are used in (76), (77), and (78), the presence of such divisors in them, satisfying the imposed conditions, as are not included in the systems of least divisors does not affect the results.

Form of n.	r.	Conditions for ν.	$\overset{n}{\underset{1}{T}}\left[\breve{\bar{\mathrm{c}}}\,(d=\hat{n})\,.\left(\frac{n}{d}=r_3\right)\right]^2.$
$3i\pm1$	±1	$\mathrm{c}\,\hat{n}\,.\,1_3$	$\overset{n}{\underset{1}{T}}[\breve{\bar{\mathrm{c}}}\,(\hat{n}\,.\,1_3)]^2$
	∓1	$\mathrm{c}\,\hat{n}\,.\,2_3$	$\overset{n}{\underset{1}{T}}[\breve{\bar{\mathrm{c}}}\,(\hat{n}\,.\,2_3)]^2$
	0	No such ν	n^2
$3^g(3i\pm1)$	±1	$\mathrm{c}\,3^g$	$\overset{n}{\underset{1}{T}}[\breve{\bar{\mathrm{c}}}\,3^g]^2$
	∓1	$\mathrm{c}\,3^g\,.\,(\hat{n}\,.\,2_3)$	$\overset{n}{\underset{1}{T}}[\breve{\bar{\mathrm{c}}}\,3^g\,.\,(\hat{n}\,.\,2_3)]^2$
$3^g(3i\pm1)$ $g>1$	0	$\mathrm{c}\,\hat{n}$	$\tau^2(n)$
$3^g(3i\pm1)$ $g=1$	0	$\mathrm{c}\,(\hat{n}\,.\,\bar{0}_3)$	$\overset{n}{\underset{1}{T}}[\breve{\bar{\mathrm{c}}}\,(\hat{n}\,.\,\bar{0}_3)]^2$

(79)

where the upper or lower sign is to be used throughout any line in which the double sign occurs. Another example is given in (55).

Let $\lambda, \mu, \nu, \ldots.$ be any numerical quantities, positive or negative, and $\epsilon_1, \epsilon_2, \epsilon_3, \ldots.$, any succession of the signs $+$ and $-$ (or of the quantities $+1$ and -1); and let

$$\sigma=\epsilon_1\lambda+\epsilon_2\mu+\epsilon_3\nu+\ldots., \text{ and } [f(\;)]\,\sigma=\epsilon_1 f(\lambda)+\epsilon_2 f(\mu)+\epsilon_3 f(\nu)+\ldots.; \tag{80}$$

then I call $[f(\;)]\,\sigma$ *a functional distribute.* What is essential to the definition of a functional distribute is the manner in which σ is made up of terms $\lambda, \mu, \nu, \ldots.$, and the sign prefixed to each; i.e. the *form of expression* of σ is essential. In the cases which I have occasion to consider here the expression σ is the complete development of an integral algebraic expression, the terms $\lambda, \mu, \nu, \ldots.$ being taken all positive, and therefore $\epsilon_1, \epsilon_2, \epsilon_3, \ldots.$, are the signs actually occurring in the development. For the sake of brevity I write, in these cases, σ in its undeveloped form. Thus, $\tau(n)$ being assumed of the form given in (76),

$$[f(\;)]\,\tau(n)=f(n)-f\left(\frac{n}{a}\right)-f\left(\frac{n}{b}\right)-f\left(\frac{n}{c}\right)-\ldots.+f\left(\frac{n}{ab}\right)+f\left(\frac{n}{ac}\right)+f\left(\frac{n}{bc}\right)$$
$$+\ldots.-f\left(\frac{n}{abc}\right)-\ldots., \tag{81}$$

$$[f(\ )]\left(\frac{1-a^{\alpha+1}}{1-a}\right)\left(\frac{1-b^{\beta+1}}{1-b}\right)\left(\frac{1-c^{\gamma+1}}{1-c}\right)\ldots\ldots=[f(\ )]\,(1+a+a^2+\ldots\ldots$$
$$+a^{\alpha})\,(1+b+b^2+\ldots\ldots+b^{\beta})\,(1+c+c^2+\ldots\ldots+c^{\gamma})\ldots\ldots$$
$$=f(1)+f(d)+f(d')+\ldots\ldots+f(n), \tag{82}$$

where $a, b, c, \ldots\ldots, \alpha, \beta, \gamma, \ldots\ldots, d, d', \ldots\ldots$ are defined as above.

Professor Sylvester has called the function $[f(\ )]\tau(n)$ the *functional totient* of $f(n)$ and

$$[f(\ )]\left(\frac{1-a^{\alpha+1}}{1-a}\right)\left(\frac{1-b^{\beta+1}}{1-b}\right)\ldots\ldots$$

the *functional summant* of $f(n)$, and has denoted them by $(f\tau)n$ and $(f\sigma)n$, respectively (this Journal, Vol. II. pp. 386, 387).

List of Articles relating to the Subject of the foregoing Paper.

Cayley, A.: On Residuation in regard to a Cubic Curve. Messenger of Mathematics, 2d ser., III. pp. 62 – 65.

Cayley, A.: On the Problem of the in- and circumscribed Triangle. Phil. Trans., CLXI. pp. 369 – 412; Proc. Royal Soc., XIX. p. 292.

Clebsch, A.: Vorlesungen über Geometrie. I. Band. Herausgegeben von F. Lindemann. Leipzig, 1876. [5te Abtheilung: Die Curven dritter Ordnung und dritter Klasse. pp. 497 – 660.]

Clebsch, A.: Ueber einen Satz von Steiner und einige Punkte der Theorie der Curven dritter Ordnung. Crelle's Journal, LXIII.

Clebsch, A.: Ueber diejenigen ebenen Curven, deren Coordinaten sich als elliptische Functionen eines Parameters darstellen lassen. Crelle's Journal, LXIV.

Durège, H.: Ueber fortgesetztes Tangentenziehen an Curven dritter Ordnung mit einem Doppel- oder Rückkehrpunkte. Math. Annalen, I. pp. 509 – 532.

Guessfeldt: Diss. inaug. de curva plana. Bonn, 1865.

Harnack, A.: Ueber die Verwerthung der elliptischen Functionen für die Geometrie der Curven dritten Grades. Math. Annalen, IX. pp. 1 – 54.

Igel, B.: Ueber ebene Curven dritter Ordnung mit einem Doppelpunkt. Math. Annalen, VI. pp. 633 – 642.

Rosenow, H.: Die Curven dritter Ordnung mit einem Doppelpunkt, nach den Methoden der neueren Algebra (Invariantentheorie) behandelt. [Dissertation.] Breslau, 1873.

Salmon, G.: A Treatise on the higher Plane Curves: Intended as a Sequel to a Treatise on Conic Sections. 2d ed. Dublin, 1873. pp. 133 – 136, 176 – 178, 180, 181.

Sturm, R.: Ueber die ebenen Curven dritter Ordnung. Crelle's Journal, XC. pp. 85 – 101 [especially pp. 97, 100].

Sylvester, J. J.: On Certain Ternary Cubic-form Equations. Amer. Jour. Math., III. pp. 58 – 88, 184 – 189.